eSecurity

Treinamentos em Segurança da Informação

O que temos para hoje?

Menu do dia:

- ✓ **HIDS**
  - ✓ O que é um HIDS
  - ✓ Principais Funções
  - ✓ Vantagens
  - ✓ OSSEC
  - ✓ Métodos de trabalho
  - ✓ Client x Server
- ✓ **Mão na massa**
  - ✓ HIDS: Instalação local
  - ✓ HIDS: Manipulando serviços
  - ✓ Instalando OSSEC WUI

O HIDS

O que é um HIDS

Sistemas Hospedeiros de Detecção de Intrusos e Sistemas de Rede de Detecção de Intrusos, ou HIDs e NIDs (respectivamente, os acrônimos originais, em inglês), são sistemas computadorizados de segurança de rede utilizados para proteção contra vírus, spyware, malware e outros tipos maliciosos de arquivo.

A diferença é que os HIDs (Sistemas Hospedeiros de Detecção de Intrusos) são instalados somente em certos pontos de interseção, como servidores e roteadores, por exemplo, enquanto os NIDs (Sistemas de Rede de Detecção de Intrusos) são instalados em todas as máquinas hospedeiras.

Embora firewalls e programas contra malwares possam servir bem para computadores individuais, falta a eles a inteligência necessária para defender uma rede corporativa.

Por exemplo, HIDs e NIDs coletam informações de uma rede e comparam-nas com padrões pré-determinados para descobrir ataques e vulnerabilidades, além de criarem bancos de dados de normalidade de comportamento.

HIDS: Funções Principais

Os HIDs examinam ações específicas com base em hospedeiros, como, por exemplo, os aplicativos que estão sendo utilizados, os arquivos que estão sendo acessados e as informações que residem nos logs de kernel.

Os NIDs analisam o fluxo de informações entre computadores, ou seja, o tráfego da rede. Essencialmente, "farejam" um comportamento suspeito na rede.

Dessa forma, os NIDs podem detectar um hacker antes que possa haver uma invasão, enquanto que os HIDs só poderão detectar problemas depois de o hacker já ter violado o sistema.

HIDS: Vantagens

Embora, a princípio, os HIDs possam parecer uma solução ruim, reúnem diversas vantagens. Por exemplo, podem impedir que ataques resultem em danos.

Se um arquivo malicioso tentar reescrever um arquivo, o HID pode limitar seus privilégios e colocá-lo em quarentena.

Os HIDs podem proteger notebooks ao serem retirados de uma rede e levados para o campo.

Em última análise, os HIDs são uma ferramenta de "última linha de defesa", utilizada para repelir os ataques não detectados pelo NID.

Fonte: EHOW

HIDS: OSSEC

O OSSEC é um HIDS que tem muitas funcionalidades, ele tem a capacidade de trabalhar localmente, ou trabalhar em uma rede, como cliente e servidor.

Uma das grandes vantagens dos OSSEC, é que trabalha com Active Response, ou seja, para determinados tipos de ataques, ele pode tomar algumas medidas, como bloquear o IP que está atacando por um determinado tempo e mandar um e- mail alertando sobre o ocorrido.

O OSSEC é multiplataforma, portanto, você poderá instala-lo em máquinas Windows Server e Linux, de acordo com as necessidades da sua rede.

O OSSEC monitora o registro do Windows e detecta qualquer alteração e registra.

HIDS: Métodos de trabalho

O OSSEC trabalha com 3 métodos de trabalho:

Local – Onde são perguntados todos os parâmetros de configuração do OSSEC Análise de log, análise de integridade, análise de rootkit, alerta em tempo real e efetua respostas ativas (Bloqueios, por exemplo)

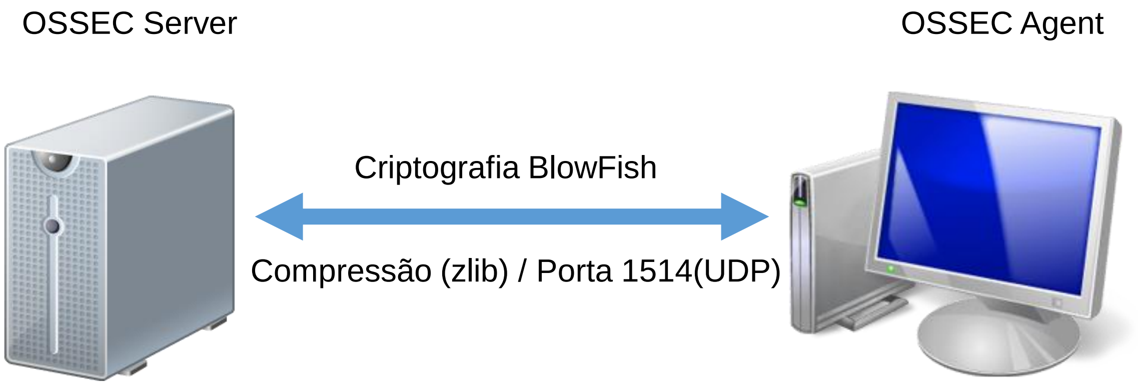
Cliente – Neste método ele efetua Análise de log, análise de integridade, análise de rootkit, porém, envia essas análises ao servidor para que ele tome a ação

Servidor – Faz tudo o que o método local faz e também é capacitado a receber os logs dos clientes.

HIDS: Client x Server

O **OSSEC** trabalha também em processo Client x Servidor, esse método é melhor utilizado em redes que demandam alta performance, pois, são analisados apenas os dados setados pelo administrador.

A comunicação entre cliente x Servidor é criptografada com a tecnologia blowfish



Colocando em prática

HIDS: Instalação Local

Após a instalação do sistema operacional Ubuntu Server, são seguidos os seguintes passos e instalações:

```
# Atualização do repositório
sudo apt-get update
# Instalação dos compiladores básicos
sudo apt-get install build-essential
# Download do HIDS
wget -U ‘Mozilla' http://www.ossec.net/files/ossec-hids-2.7.1.tar.gz
# Descompactação do arquivo
tar –zxvf ossec-hids-2.7.1.tar.gz
# Acesso na pasta descompactada
cd ossec-hids-2.7.1
# Execute o script de instalação
./install.sh
```

HIDS: Instalação Local

Você precisará responder algumas perguntas durante a instalação. São elas:

Atualização do repositório

Para instalação em português, escolha [br]

```
1- Que tipo de instalação você deseja (servidor, cliente, local ou ajuda)? local

  - Escolhida instalação local.

2- Configurando o ambiente de instalação.

 - Escolha onde instalar o OSSEC HIDS [/var/ossec]:

    - A instalação será feita no diretório /var/ossec .

3- Configurando o OSSEC HIDS.

  3.1- Deseja receber notificações por e-mail? (s/n) [s]: n

   --- Notificação por e-mail desabilitada.

  3.2- Deseja habilitar o sistema de verificação de integridade? (s/n) [s]: s

   - Syscheck (Sistema de verificação de integridade) habilitado.

  3.3- Deseja habilitar o sistema de detecção de rootkis? (s/n) [s]: s

   - Rootcheck (Sistema de detecção de rootkits) habilitado.
```

HIDS: Instalação Local

Perceba que a instalação inteira é feita em Português e ela explica os itens ao qual você fará as escolhas

```
3.4- Respostas automáticas permitem você executar um comando
     específico baseado nos eventos recebidos. Você pode
     bloquear um endereço de IP ou desabilitar o acesso de
     um usuário específico, por exemplo.
     Maiores informações:
     http://www.ossec.net/en/manual.html#active-response

  - Deseja habilitar o sistema de respostas automáticas? (s/n) [s]: s

  - Sistema de respostas automáticas habilitado.

  - Por padrão, nós podemos habilitar o 'host-deny' e
    o 'firewall-drop'. O primeiro adicionará um host
    ao /etc/hosts.deny e o segundo bloqueará o host
    no 'iptables' (se linux) ou no ipfilter (se Solaris,
    FreeBSD ou NetBSD).
  - Eles podem ser usados para parar 'SSHD brute force
    scans', portscans e outras formas de ataque.
    Você pode também realizar  bloqueios baseados nos
    alertas do snort, por exemplo.

  - Deseja habilitar o firewall-drop? (s/n) [s]: s

    - firewall-drop habilitado (local) para níveis >= 6
```

HIDS: Instalação Local

Você também poderá adicionar IPs na White list, para que não bloqueie. Isso é útil para redes internas ou ambientes conhecidos.

```
  - Lista de endereços que não serão bloqueados pela resposta automática:
     - 187.122.127.34
     - 187.122.127.58

  - Deseja adicionar mais algum endereço a essa lista? (s/n)? [n]:

 3.6- Ajustando a configuração para analisar os seguintes logs:
   -- /var/log/auth.log
   -- /var/log/syslog
   -- /var/log/dpkg.log

- Se quiser monitorar qualquer outro arquivo, modifique
  o ossec.conf e adicione uma nova entrada para o arquivo.
  Qualquer dúvida sobre a configuração, visite http://www.ossec.net/hids/ .


  --- Pressione ENTER para continuar ---
```

HIDS: Instalação Local

No fim da instalação, o sistema lhe apresentará a mensagem abaixo:

```
cp -pr ossec-monitord ../../bin
cp -pr ossec-reportd ../../bin
make[1]: Leaving directory `/home/alan/ossec-hids-2.7.1/src/monitord'
make[1]: Entering directory `/home/alan/ossec-hids-2.7.1/src/os_auth'
cp -pr ossec-authd ../../bin
cp -pr agent-auth ossec-authd ../../bin
make[1]: Leaving directory `/home/alan/ossec-hids-2.7.1/src/os_auth'


 - O Sistema é Debian (Ubuntu or derivative).
 - O script de inicialização foi modificado para executar o OSSEC HIDS durante o
 boot.

 - Configuração finalizada corretamente.

 - Para iniciar o OSSEC HIDS:
                /var/ossec/bin/ossec-control start

 - Para parar o OSSEC HIDS:
                /var/ossec/bin/ossec-control stop

 - A configuração pode ser vista ou modificada em /var/ossec/etc/ossec.conf


    Obrigado por usar o OSSEC HIDS.
    Se você tiver alguma pergunta, sugestão ou encontrar algum
    "bug", nos contate através do e-mail contact@ossec.net ou
    utilize nossa lista de e-mail:
    ( http://www.ossec.net/main/support/ ).

    Maiores informações podem ser encontradas em http://www.ossec.net

    ---  Pressione ENTER para continuar  ---
```

HIDS: Manipulando serviço

Para manipular o serviço do OSSEC e acompanhar suas detecções, siga os seguintes passos:

\# Iniciar o serviço
/var/ossec/bin/ossec-control start

\# Parar o serviço
/var/ossec/bin/ossec-control stop

\# Ler logs de alerta
tail –f /var/ossec/logs/alerts/alerts.log

HIDS: Instalando OSSEC WEB UI

O Ossec-WUI (Web User Interface) é uma ferramenta web que centraliza as informações sobre o servidor do Ossec HIDS e de seus agentes.
Ele possui informações em tempo real de alertas, estatísticas e etc.
A instalação do Ossec-WUI ocorrerá na mesma máquina onde foi instalado o Ossec Server ou Local.

```
# Antes é importante instalar um servidor WEB e suas bibliotecas:
apt-get install apache2 libapache2-mod-php5 apache2-utils
# Acessar a pasta onde foi instalado o servidor WEB
cd /var/www/html
# Efetuar o download o WUI
wget -U 'Mozilla' http://www.ossec.net/files/ossec-wui-0.8.tar.gz
# Descompactar o arquivo
tar -zxvf ossec-wui-0.8.tar.gz
# Renomear a pasta descompactada
tar -zxvf ossec-wui-0.8.tar.gz
# Renomear pasta para ossec
mv ossec-wui-0.8 ossec
```

HIDS: Instalando OSSEC WEB UI

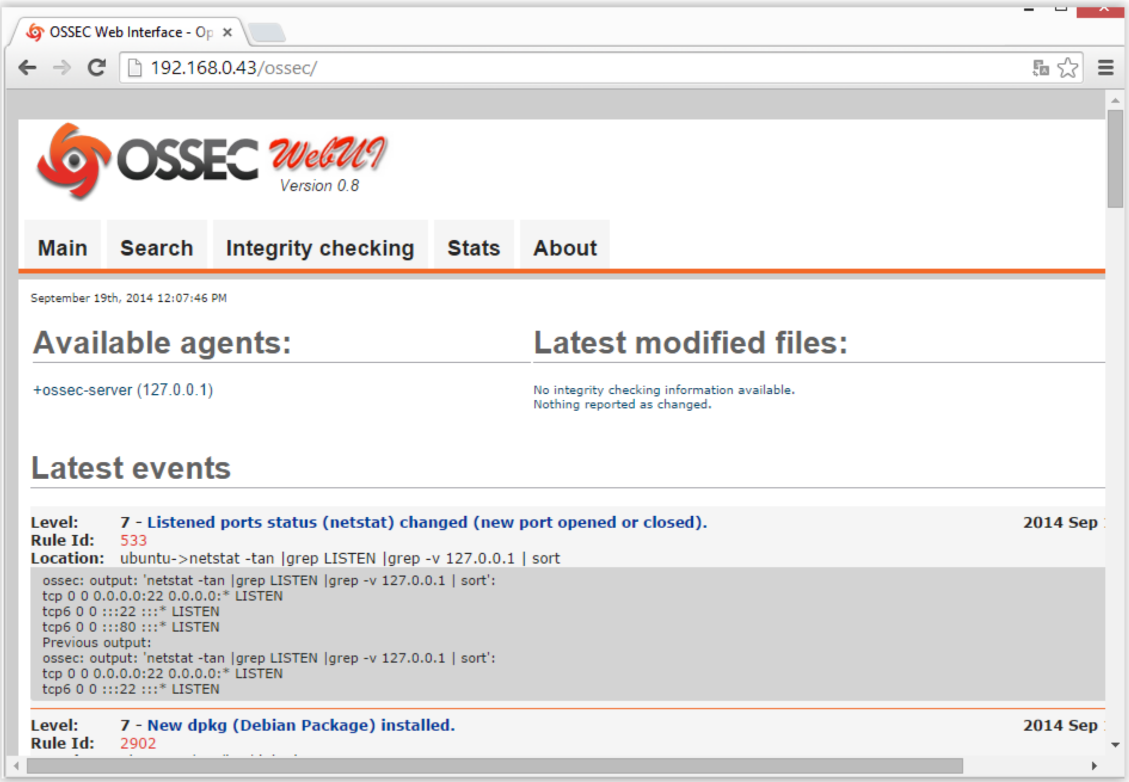
Após esse processos, também será possível instalar o ambiente utilizando um script. Antes desse processo, devemos entender que o Ubuntu utilizar o usuário www-data no sistema operacional. Caso você esteja utilizando outra distribuição, verifique qual é o usuário padrão do apache na sua distro.

Executando o script:
./ossec/setup.sh
Preencha com usuário e senha de acesso
Em seguida, será solicitado o usuário do apache, coloque www-data
Depois, a pasta onde foi instalada o OSSEC, coloque /var/ossec
A instalação foi realizada, porém, ainda não está funcional. Para isso é importante efetuar algumas liberações.
Adicione o usuário www-data no grupo ossec
usermod -a -G ossec www-data
Você pode verificar se tudo está de acordo com o comando abaixo:
cat /etc/group |grep ossec
Você deve ver algo mais ou menos assim: ossec:x:1001:www-data

HIDS: Instalando OSSEC WEB UI

Agora você precisa reiniciar os serviços e começar a monitorar através da WEB.

service apache2 restart
/var/ossec/bin/ossec-control start



Chega por hoje

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker